AMENDMENTS TO THE CLAIMS

Please cancel claims 23-26, amend claims 1, 3, 9-11, 14, 19, 21, and 22, and insert new claims 32-42, as follow. A complete listing of the claims is provided, as follows.

1. (Currently Amended) A device for managing network traffic flow, the device comprising:
a processor, the processor configured to
receive network traffic content,
determine whether a protocol of the network traffic content matches a prescribed protocol of network traffic content that could contain content desired to be detected, ~~and~~
store the network traffic content in a stack when the protocol of the network traffic content matches the prescribed protocol, wherein the stack is associated with a module configured to determine whether the network traffic content contains content desired to be detected, and
send at least a portion of the network traffic content to a memory when the protocol of the network traffic content matches the prescribed protocol.

2. (Original) The device of claim 1, wherein the processor comprises a general purpose processor.

3. (Currently Amended) The device of claim 1, wherein the ~~special purpose~~ processor comprises an ASIC processor.

4. (Original) The device of claim 3, wherein the ASIC processor is a semi-custom ASIC processor.

5. (Original) The device of claim 3, wherein the ASIC processor is a programmable ASIC processor.

6. (Original) The device of claim 1, wherein the processor is further configured to send the network traffic content to a user when the protocol of the network traffic content does not match the prescribed protocol.

7. (Original) The device of claim 1, further comprising the stack.

8. (Original) The device of claim 7, wherein the stack is implemented in the processor or in another processor.

9. (Currently Amended) The device of claim 8, wherein the stack is configured to store the network traffic content in accordance with the protocol of the network traffic content.

10. (Currently Amended) The device of claim 1, ~~further comprising a memory;~~ wherein the processor is further configured to

~~send at least a portion of the network traffic content to the memory when the protocol of the network traffic content matches the prescribed protocol,~~

~~send a copy of the network traffic content to a module, the module configured to determine whether the network traffic content contains content desired to be detected,~~ ~~and~~

assemble the at least a portion of the network traffic content with the rest of the network traffic content, and transmit the network traffic content to a user when it is determined that the network traffic content does not contain the content desired to be detected.

11. (Currently Amended) The device of claim ~~10~~ 1, further comprising the module.

12. (Original) The device of claim 11, wherein the module is implemented in the processor.

13. (Original) The device of claim 11, wherein the module is implemented in an ASIC processor.

14. (Currently Amended) The device of claim 1, ~~further comprising a memory;~~ wherein the processor is further configured to

flag the network traffic content when the protocol of the network traffic content matches the prescribed protocol, and

send the flagged network traffic content to the memory~~;~~

~~send a copy of the network traffic content to a module, the module configured to determine whether the network traffic content contain content desired to be detected, and~~

~~transmit the network traffic content to a user when it is determined that the network traffic content does not contain the content desired to be detected~~.

15. (Original) The device of claim 14, further comprising the module.

16. (Original) The device of claim 15, wherein the module is implemented in the processor.

17. (Original) The device of claim 15, wherein the module is implemented in an ASIC processor.

18. (Original) The device of claim 1, wherein the content desired to be detected is selected from the group consisting of a virus, a worm, a web content, a Trojan agent, an email spam, and a packet transmitted by a hacker.

19. (Currently Amended) A method for managing network traffic flow, the method comprising:

receiving network traffic content;

determining whether a protocol of the network traffic content matches with a prescribed protocol of network traffic content that could contain content desired to be detected; ~~and~~

storing the network traffic content in a stack when the protocol of the network traffic content matches the prescribed protocol, the stack associated with a module configured to determine whether the network traffic content contain content desired to be detected; and

sending at least a portion of the network traffic content to a memory when the protocol of the network traffic content matches the prescribed protocol.

20. (Original) The method of claim 19, wherein the network traffic content is stored in the stack in accordance with the protocol of the network traffic content.

21. (Currently Amended) The method of claim 19, further comprising:

~~sending at least a portion of the network traffic content to a memory when the protocol of the network traffic content matches the prescribed protocol;~~

~~sending a copy of the network traffic content to a module, the module configured to determine whether the network traffic content contain content desired to be detected, and~~

assembling the at least a portion of the network traffic content with the rest of the network traffic content, and sending the network traffic content to a user when it is determined that the network traffic content does not contain the content desired to be detected.

22. (Currently Amended) The method of claim 19, further comprising:

flagging the network traffic content when the protocol of the network traffic content matches the prescribed protocol; and

storing the flagged network traffic content in a memory;

~~sending a copy of the network traffic content to a module, the module configured to determine whether the network traffic content contain content desired to be detected, and~~

~~transmitting the network traffic content to a user when it is determined that the network traffic content does not contain the content desired to be detected~~.

23-26. (Canceled).

27. (Original) A device for managing network traffic flow, the device comprising:

a first processor, the first processor configured to

receive network traffic content,

flag the network traffic content,

send the flagged network traffic content to a module, the module configured to pass unflagged data to a user and prevent flagged data from being sent to the user, and

send a copy of the network traffic content to a second processor, the second processor configured to determine whether the network traffic content contains content desired to be detected.

28. (Original) The device of claim 27, wherein the first processor is further configured to transmit the network traffic content to a user when it is determined that the network traffic content does not contain the content desired to be detected.

29. (Original) The device of claim 27, wherein the module comprises a memory, a buffer, or at least a portion of a processor.

30. (Original) A method for managing network traffic flow, the method comprising:

receiving network traffic content;

flagging the network traffic content;

sending the flagged network traffic content to a module, the module configured to pass unflagged data to a user and prevent flagged data from being sent to the user; and

sending a copy of the network traffic content to a processor, the processor configured to determine whether the network traffic content contains content desired to be detected.

31. (Original) The method of claim 30, further comprising transmitting the network traffic content to a user when it is determined that the network traffic content does not contain the content desired to be detected.

32. (New) The device of claim 1, further comprising the memory.

33. (New) The device of claim 27, wherein the first processor is configured to pass a portion of the network traffic content downstream before the second processor finishes processing the network traffic content.

34. (New) The device of claim 27, wherein the first processor and the second processor are parts of a processor.

35. (New) The device of claim 34, wherein the processor comprises an ASIC processor.

36. (New) The device of claim 27, wherein the first processor is configured to flag the network traffic content by modifying data associated with the network traffic content or by inserting data to the network traffic content.

37. (New) The method of claim 30, wherein a portion of the network traffic content is passed downstream before the processor finishes processing the network traffic content.

38. (New) The method of claim 30, wherein the processor comprises an ASIC processor.

39. (New) The method of claim 30, wherein the network traffic content is flagged by modifying data associated with the network traffic content or by inserting data to the network traffic content.

40. (New) A device for managing network traffic flow, the device comprising:
a processor, the processor configured to
receive network traffic content,
pass a first portion of the network traffic content downstream, and
pass a second portion of the network traffic content to a stack for allowing the second portion to be scanned for content that is desired to be detected.

41. (New) The device of claim 40, wherein the processor is further configured to pass the second portion downstream after the second portion is scanned.

42. (New) The device of claim 40, wherein the first portion of the network traffic content is not scanned for the content that is desired to be detected.